REMARKS

The present response is intended to be fully responsive to the rejection raised in the Office action, and is believed to place the application in condition for allowance. Further, the Applicant does not acquiesce to any portion of the Office Action not particularly addressed. Favorable reconsideration and allowance of the application is respectfully requested.

In the Office action, the Office noted that claims 1-16 are pending and rejected. Applicants amend claims 1-13 and cancel claims 2 and 14. Applicant has not introduced any new matter by way of the foregoing amendments.

In view of the above amendments and the following discussion, the Applicant submits that none of the claims now pending in the application are obvious under the provisions of 35 U.S.C. § 103. Furthermore, Applicants submit that all pending claims comply with 35 U.S.C. § 101 and 35 U.S.C. § 112. Thus, Applicant believes that all of these claims are now in condition for allowance.

OBJECTION

The Office objected to claims 1 and 13 for failing to recite that the matrix is a square matrix. Applicant amends claims 1 and 13 to remedy the anomaly. Therefore, Applicant requests reconsideration and withdrawal of the objection to claims 1 and 13.

REJECTION

The Office rejected claims 1 and 13 under 35 U.S.C. § 112 and claims 1-16 and 13 under 35 U.S.C. § 101. In addition, the Office rejected claims 9-12 and 15-16 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 4,322,577 issued to Brandstorm et al. (hereon after "Brandstorm") in view of U.S. Patent Publication No. 2003/0016823 published to Chen et al. (hereon after "*Chen*") and claims 9-12 and 15-16 over U.S. Patent Publication No. 2003/0028484 published to Boylan et al. (hereon after "*Boylan*") in view of U.S. Patent No. 4,322,577 issued to Brandstorm et al. (hereon after "Brandstorm"). The Applicant respectfully traverses the rejections.

A. Applicant's Response to the 35 U.S.C. § 112 Rejection of claims 1 and 13

Office rejected claims 1 and 13 for being incomplete for omitting essential steps. The Office indicated that the omitted steps are "1) a preprocessing random permutation of the data (message0 and 2) when the determinant of matrix is 0 or 1, then exit the procedure by returning "encryption failed" and try the encryption again with a new set of fields (e.g., a new time stamp in the message)."

Applicants amend claims 1 to recite "A method of encryption, of a digital signal processor, comprising, preprocessing said input message wherein said preprocessing includes a permutation of said input message; partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix; computing a determinant of said matrix; public key encrypting said determinant; and multiplying said matrix by said encrypted determinant." Claims 13 has been amended to recite similar features as those recited in claim 1.

Thus, Applicants respectfully request reconsideration and withdrawal of the rejection to claims 1 and 13.

B. Applicant's Response to the 35 U.S.C. § 101 Rejection of claims 1-16

Office rejected claims 1-16 for reciting an invention that is directed to a non-statutory subject matter. Applicants amend claims 1, 9 and 13 specifically to recite a method "for a digital signal processor." Thus, reconsideration and withdrawal of the rejection to claims 1-16 is respectfully requested.

C. Applicant's Response to the 35 U.S.C. § 103(a) Rejection of claims 1-8 and 13-14

The Office rejected claims 1-8 and 13-14 under 35 U.S.C. § 102(b) as being unpatentable over *Brandstorm*. The Applicant traverses the rejection.

As the Examiner is aware, "anticipation requires the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim." *Lindemann Maschinen Fabrick GmbH v. American Hoist Derrick Co.*, 221 USPQ 481, 485 (Fed. Cir. 1984) [emphasis added]. Applicant

submits that the cited reference is devoid from disclosing at least one element recited in Applicant recited invention.

Applicants amend claim 1 to better describe Applicants' inventive concept. Amended claim 1 recites a combination of elements directed to a method of encryption. The combination of elements includes "preprocessing said input message wherein said preprocessing includes a permutation of said input message; partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix; computing a determinant of said matrix; public key encrypting said determinant; and multiplying said matrix by said encrypted determinant."

Brandstorm discloses an encryption and decryption method and apparatus, in which a plaintext message blocks and sublocks "are interpreted as elements of Galois-field [and a] plaintext matrix (M) of said elements is multiplied by a first key matrix (A) of a group of Galois-field, the resulting product (M.A) being multiplied by a second key matrix (B) of the same group over said Galois-field." *Brandstorm,* at Abstract. *Brandstorm* discloses "a plaintext message applied as blocks m consisting of, for example, data bots to a matrix encoder 1. The output of the encoder delivers a matrix M for each block m. The elements in the matrix M belong to a Galois-field… These matrices are supplied to a matrix multiplier 42… also the matrix encoder 42 may be a part of a common matrix encoder 40, 41" *Id.* at col. 6 lines 4-63.

Chen, on the other hand, discloses a method for encrypting data comprising dividing a first data set into a second data set and a third data set; deriving a first value using the second data set as an input into a polynomial equation; deriving a second value using the third data set as an input into the polynomial equation; deriving a first encryption key associated with a second party; encrypting the first value with the first encryption key; encrypting the second value with the second encryption key." As such, *Chen* requires utilizing 3 data sets and two encryption keys. Consequently, Applicants submit that *Chen* teaches away from *Brandstorm*.

Furthermore, Applicants submit that *Brandstorm* and *Chen*, alone and in combination, are devoid from disclosing all the elements recited in amended claim 1, which includes "preprocessing said input message wherein said preprocessing includes a permutation of said input message; partitioning said input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix; computing a determinant of said matrix; public key encrypting said

determinant; and multiplying said matrix by said encrypted determinant." Amended claim 13 recites similar features as those recited in claim 1. Hence, claims 1 and 13, in view of *Brandstorm* and *Chen*, alone and in combination, satisfy the requirements of 35 U.S.C. § 103(a) and is in condition for allowance.

Claims 2-8 and 14 depend, directly or indirectly, from claims 1 and 13, respectively, and, thus, necessarily contain each and every element recited in their respective independent claim. Since the Applicant submits that *Brandstorm* and *Chen*, alone and in combination, do not deem claims 1 and 13 obvious, the Applicant further submits that *Brandstorm* and *Chen*, alone and in combination, also do not deem claims 2-8 and 14 obvious. Hence, claims 1-8 and 13-14 satisfy the requirements of 35 U.S.C. § 103(a) and are in condition for allowance.

The Office rejected claims 9-12 and 15-16 under 35 U.S.C. § 103(a) as being unpatentable over *Boylan* in view of *Brandstorm*.

Boylan discloses "a method for inter-terminal payment and corresponding devices and computer programs loadable into said devices [wherein] the method comprises a transfer of financial velue from a payment device of a payer (PDPr) to a payment device of payee (PDPe) with the assistance and the supervision of a trusted third party (TTP) by a message. *Boylan*, at Abstract. Chen, on the other hand, "techniques over the conventional random number generators and radomizatiom procedures [that uses] irrational numbers over pseudo-random numbers generated by LFSR…." *Chen*, at Abstract.

Brandstorm discloses an encryption and decryption method and apparatus, in which a plaintext message blocks and sublocks "are interpreted as elements of Galois-field [and a] plaintext matrix (M) of said elements is multiplied by a first key matrix (A) of a group of Galois-field, the resulting product (M.A) being multiplied by a second key matrix (B) of the same group over said Galois-field." *Brandstorm,* at Abstract. *Brandstorm* discloses "a plaintext message applied as blocks m consisting of, for example, data bots to a matrix encoder 1. The output of the encoder delivers a matrix M for each block m. The elements in the matrix M belong to a Galois-field… These matrices are supplied to a matrix multiplier 42… also the matrix encoder 42 may be a part of a common matrix encoder 40, 41" *Id.* at col. 6 lines 4-63.

Applicants amend claims 9 to recite "preprocessing said input message wherein said preprocessing includes a permutation of said input message and defining a permutation source; generating a permuted message for an input

message employing said permutation source; padding said permuted message with said permutation source to obtain a preprocessed message; and encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message." Amended claim 13 recites similar features as those recited in amended claim 9.

Applicants submit that *Boylan* and *Brandstorm*, alone and in combination, are devoid from disclosing all the elements recited in amended claims 9 and 13. Given that each of the dependent claims 10-12 and 15-16 depend, directly or indirectly, from independent claims 9 and 13, respectively, each necessarily includes all the elements of its respective independent claim.

Since Applicant submits that *Boylan* and *Brandstorm*, alone and in combination, do not disclose all the elements or render claims 9 and 13 obvious, the Applicant further submits that *Boylan* and *Brandstorm,* alone and in combination, also do not disclose all the elements or render claims 10-12 and 15-16 obvious. The Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 9-12 and 15-16.

CONCLUSION

In view of the foregoing, the Applicants submit that none of the claims presently in the application are obvious under the provisions of 35 U.S.C. §103. Furthermore, Applicants submit that all pending claims comply with 35 U.S.C. § 101 and 35 U.S.C. § 112. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Office believes that any unresolved issues still exist or if, in the opinion of the Office, a telephone conference would expedite passing the present application to issue, the Office is invited to call the undersigned attorney directly at 972-917-4365 or the office of the undersigned attorney at 972-917-4363 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

Date: March 20, 2009

By: /Mirna Abyad/
MIRNA ABYAD
Registration No. 58,615
Texas Instruments Incorporated
P.O. Box 655474, M/S 3999
Dallas, TX 75265
Telephone: (972) 917-4365